



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,042	03/30/2001	Juan A. Garay	7-42-7-29	1008

22046 7590 07/14/2005

LUCENT TECHNOLOGIES INC.
DOCKET ADMINISTRATOR
101 CRAWFORDS CORNER ROAD - ROOM 3J-219
HOLMDEL, NJ 07733

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT PAPER NUMBER

2137

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/823,042

Applicant(s)

GARAY ET AL.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated April 18, 2005 with the amendments to claims 1, 3, 16-17, 25-26, 33-34 and 36.

Claims 1-44 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-44 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments focus on the combination of features introduced by the amendment with elements that already existed in the claims. The new material is rendered obvious by Spies et al. (6,055,314), Shona et al. (6,018,581), Jaffe et al. (6,510,518), Otway et al. (2004/0205344), Novoa et al. (6,493,824) and Richards (6,385,723).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2137

4. Claims 1-3, 5, 12-17, 24-26, 31-32, 34-36 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al. (6,055,314) in view of Shona et al. (6,018,581).

a) As to claims 1 and 16, Spies discloses systems and methods for secure purchase and delivery of video content programs over various distribution media including a cryptographic key store for storing a transformed cryptographic key and accessing circuitry for accessing the transformed crypto key from the crypto key store (col. 5, lines 40-44; Fig. 3) comprising the step of storing key re-transforming information for the transformed crypto key in a decryption store (col. 3, lines 5-18), the accessing circuitry being able to communicate with the decryption store exclusively via a predetermined interface, (Fig. 6, element 112; Figs. 7-8) the interface being such that the accessing circuitry is unable to access from the decryption store at least one of: at least a portion of the key re-transforming information and at least a portion of the cryptographic key (col. 2, lines 34-42; col. 3, lines 65-67 to col. 4, lines 1-2).

However, Spies does not disclose the key re-transforming information has a transformation pattern randomly generated by the decryption store.

Shona discloses a communication system for maintaining high security in communication between a communication apparatus and a terminal (IC card) comprising the key re-transforming information (Fig. 1, element Y1) has a transformation pattern randomly generated (Fig. 1, element R2) by the decryption store (Fig. 1, element 12).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of key re-transforming information has a transformation pattern randomly generated by the decryption store in the system of Spies as Shona teaches so as to strengthen security in communication system.

b) As to claim 2, 17, 26 and 35, Spies as modified discloses the interface is such that the accessing circuitry is unable to access from the decryption store both of: at least a portion of the key re-transforming information (col. 2, lines 39-42) and at least a portion of the cryptographic key (col. 3, line 67 to col. 4, line 1; col. 5, lines 48-49; col. 10, lines 62-64).

c) As to claims 3 and 36, Spies as modified discloses the key re-transforming information comprises a key decrypting algorithm (Fig. 6, element 118),

d) As to claims 5, 24, 31 and 38, Spies as modified discloses the method further comprising the steps of the decryption store receiving the crypto key (col. 10, lines 37-39), the decryption store transforming the cryptographic key using key transforming information to produce the transformed crypto key (col. 10, lines 39-45) and the decryption store sending the transformed crypto key to the crypto key store (col. 10, lines 45-48).

e) As to claim 12, Spies as modified discloses the accessing circuitry's communication with the decryption store comprises the transfer of information between them (Figs. 6-7).

f) As to claim 13, Spies as modified discloses storing the transformed cryptographic key in the cryptographic key store for a period of time (col. 11, lines 20-

Art Unit: 2137

25), the decryption depends upon the packet key and decryption information changes every packet, or approximately every 300ms anticipate crypto key is stored for a period of time.

g) As to claims 14-15, Spies as modified discloses the step of erasing the crypto key from the decryption store at the completion of each crypto operation (col. 10, line 45) and the crypto key is stored in the decryption store in such a way that it disappears from the decryption store when the decryption store is removed from the system (col. 10, lines 46-48).

h) As to claims 25 and 34, Spies as modified discloses a decryption store for storing key re-transforming information for a transformed crypto key, the decryption store comprising: a predetermine interface, the interface being operable to receive the transformed crypto key (Fig. 6, element 112) and an output port complying exclusively with the predetermined interface such that information is accessible from the decryption store through the output port wherein at least one of: at least a portion of the key re-transforming information and at least a portion of the crypto key being not accessible from the decryption store through the output port (col. 10, lines 59-64).

i) As to claim 32, Spies as modified (see claims 25 and 31), Shona discloses the transformed cryptographic key (see Shona, Fig. 1, element Y1) is a function of a transformation pattern (see Shona, Fig. 1, element R2).

Art Unit: 2137

5. Claims 4, 33 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al., (6,055,314) in view of Shona et al. (6,018,581) and further in view of Jaffe et al. (6,510,518).

Spies and Shona do not disclose the transformation pattern comprises a unique identifier of the decryption store.

Jaffe discloses cryptographic tokens that must maintain the security of secret information in hostile environments comprising a transformation pattern that is unique to decryption store (col. 1, lines 19-34).

It would have been obvious to one ordinary skill in the art at the time of the invention to employ the use of a transformation pattern as Jaffe teaches in the system of Spies and Shona so as to strengthen the security of secret information.

6. Claims 6, 18, 27 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al., (6,055,314) in view of Shona et al. (6,018,581) and further in view of Otway et al. (2004/0205344).

a) As to claims 6 and 18, Spies discloses the method wherein the cryptographic key store comprises a computer memory and accessing circuitry comprises a processor. However, Spies and Shona do not disclose the decryption store comprises a mobile terminal.

Otway discloses a smart card (subscriber identification module – SIM) plugged into the mobile phone allows storing data and decrypting messages (page 3, paragraph [0025].

It would be have been obvious to one ordinary skill in the art at the time of the invention to employ the use of mobile terminal in the decryption store as Otway teaches in the system of Spies and Shona so as to provide different types of communication interface devices to the network.

b) As to claims 27 and 39, please see the addressed above claims 6 and 18.

7. Claims 7, 19, 28 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al., (6,055,314) in view of Shona et al. (6,018,581) and further in view of Novoa et al. (6,493,824).

a) As to claims 7 and 19, Spies discloses the method wherein the cryptographic key store comprises a computer memory and accessing circuitry comprises a processor. However, Spies and Shona do not disclose the decryption store comprises a network access card.

Novoa discloses a secure system comprising a network interface card coupled between the central processing unit and the network (Fig. 2, element 117), the network interface card has decryption capabilities (Fig. 3, element 308).

It would be have been obvious to one ordinary skill in the art at the time of the invention to employ the use of network access card in the decryption store as Novoa teaches in the system of Spies and Shona so as to provide different types of communication interface devices to the network.

b) As to claims 28 and 40, please see the addressed above claims 7 and 19.

Art Unit: 2137

8. Claims 8-11, 20-23, 29-30 and 41-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al. (6,055,314) in view of Shona et al. (6,018,581) and further in view of Richards (6,385,723).

a) As to claims 8-9, 20-21, 29-30 and 41-42, Spies discloses decryption store receiving the transformed crypto key (Fig. 3, element 72).

Richards discloses an IC card system and method for securely loading an application comprising receiving the transformed crypto key and information, re-transforming the transformed crypto key to produce the crypto key (Abstract). Richards discloses two basic types of encryptions (col. 4, lines 61-67 to col. 5, lines 1-45), wherein encrypting information with crypto key and transmitting the encrypted information over the network are disclosed also (Fig. 1; col. 2, lines 7-13; col. 5, lines 53-58).

It would be have been obvious to one ordinary skill in the art at the time of the invention to employ the use of decrypting the encrypted key to obtain the crypto key and further to use the crypto key to encrypt and transmit encrypted information as Richards teaches in the system of Spies and Shona so as to securely protect transmitted data.

b) As to claims 10-11, 22-23 and 43-44, a large portion of the claim limitations are addressed in above claims 8-9, 20-21, 29-30 and 41-42. Richards further discloses the IC card decrypts the key transformation unit to obtain the transfer key, then the transfer key is used to decrypt the encrypted information and the card user could access the decrypted information (Abstract).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Application/Control Number: 09/823,042
Art Unit: 2137

Page 10

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
7/7/05

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137